Quantum Multi-Prover Interactive Proof Systems*

Keiji Matsumoto† keiji@qci.jst.go.jp

Interactive proof systems [1, 9], consist of an interaction between a computationally unbounded prover and a polynomial-time probabilistic verifier. The prover attempts to convince the verifier that a given input string satisfies some property, while the verifier tries to verify the validity of the assertion of the prover.

A multi-prover interactive proof system [3], is an extension of the (single-prover) interactive proof system in which a verifier communicates with several provers, but provers cannot communicate among themselves, nor can they know messages exchanged between the verifier and the other provers. A language L is said to have a multi-prover interactive proof system if there exists a verifier V such that (i) in case the input is in L, there exist provers $P_1, \ldots, P_k$ that can convince V with probability 1, and (ii) in case the input is not in L, no set of provers $P'_1, \ldots, P'_k$ can convince V with probability more than 1/2. The class of languages having multi-prover interactive proof systems, denoted by MIP, is equal to non-deterministic exponential time (NEXP) [2, 8].

In the multi-prover interactive proof system defined by [3], provers share some random bits. Later on, the model without shared randomness was also introduced, and this model seems also popular [2, 5, 8].

Quantum interactive proof systems were introduced by Watrous [12] in terms of quantum circuits. A consecutive work of Kitaev and Watrous [10] showed that any quantum interactive protocol, even with two-sided bounded error, can be parallelized to a three message quantum protocol with exponentially small one-sided error. They also showed that the class of languages having quantum interactive proof systems is necessarily contained in deterministic exponential time (EXP).

In this talk, we define quantum analogues of classical multi-prover interactive proof systems to include the Watrous-Kitaev's quantum single-prover model as a special case.

There are two natural quantum analogues of multi-prover interactive proof systems, because there are two different model in classical case. The classical model *with* shared randomness leads to quantum version in which provers might share entanglements at the begining of the protocol [4]. On the othre hand, the classical model *without* shared randomness leads to another quantum version, in which there is no entanglement shared by provers. In this talk, we concentrate on the latter version, which will be called simply as quantum multi-prover interactive proof system.

The first main result presented in the talk is that the class of languages having quantum multi-prover interactive proof systems, denoted by QMIP, is equal to NEXP. To our knowledge, there have been only two results that exactly characterize classical complexity classes in terms of quantum computation: one is NQP = co-$\mathrm{C_{=}P}$ result on the counting complexity by [7, 6], and the other characterizes PSPACE by PrQSPACE(*poly*), or "quantum polynomial space" [11].

Another main result we talk about deals with a special case of a single-prover quantum interactive proof system in which the prover does not have his private qubits. We call this model a *quantum oracle circuit*, since it can be regarded as a quantum counterpart of a probabilistic oracle machine [8, 2]. We prove that the class of languages that are accepted by quantum oracle circuits, denoted by QOC, is also equal to NEXP, or in other words, if the prover does not have his private qubits, the ability of the single prover system is the same as that of multi-prover system.

In additon, an overview is given about the recent results on quantum interactive proof systems.

†Quantum Computation and Information Project, ERATO, JST, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

*This talk is based on the joint work with Hirotada Kobayashi†‡

‡Department of Information Science, Graduate School of Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

References

[1] L. Babai, In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[2] L. Babai, L. Fortnow, and C. Lund. *Computational Complexity*, 1(1):3–40, 1991.

[3] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.

[4] R. Cleve, Talk at the Workshop on Quantum Computation and Information, California Institute of Technology, November 2000.

[5] U. Feige and L. Lovász, *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.

[6] S. Fenner, F. Green, S. Homer, and R. Pruim, *Proceedings of the Royal Society London A*, 455:3953–3966, 1999.

[7] L. Fortnow and J. Rogers, *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[8] L. Fortnow, J. Rompel, and M. Sipser, *Theoretical Computer Science*, 134:545–557, 1994.

[9] S. Goldwasser, S. Micali, and C. Rackoff, *SIAM Journal on Computing*, 18(1):186–208, 1989.

[10] A. Kitaev and J. Watrous, In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[11] J. Watrous, *Journal of Computer and System Sciences*, 59(2):281–326, 1999.

[12] J. Watrous, In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 112–119, 1999.